义乌广播技术应对“勒索病毒”来袭案例解析

摘　要：随着广播技术的发展，广播节目的制作和播出跟互联网的结合越来越紧密。在病毒传播越来越猖獗的今天，如何构建一个对于主持人来说几乎透明的跨网系统，同时在最大范围内保障节目的播出安全，是每个广播技术从业者面临的挑战。
关键词：勒索病毒；全台网；网闸；多倍速快录系统
中图分类号：G222　　文献标识码：A
文章编号：1671-0134（2017）11-076-03　　DOI：10.19483/j.cnki.11-4653/n.2017.11.024

文 / 方达星

1. 勒索病毒传播情况和预防要求

2017 年 5 月 12 日，一种名为“想哭”的勒索病毒袭击全球 150 多个国家和地区，影响领域包括政府部门、医疗服务、公共交通、邮政、通信和汽车制造业。勒索病毒，是一种新型电脑病毒，主要以邮件、程序木马、网页挂马的形式进行传播。一旦进入本地，就会自动运行，同时删除勒索软件样本以躲避查杀和分析。接下来，勒索病毒利用本地的互联网访问权限连接至黑客的 C&C 服务器，进而上传本机信息并下载加密私钥与公钥，利用私钥和公钥对文件进行加密。加密完成后，还会修改壁纸，在桌面等明显位置生成勒索提示文件，指导用户去缴纳赎金。这种病毒利用各种加密算法对文件进行加密，被感染者一般无法解密，必须拿到解密的私钥才有可能破解。病毒可以导致重要文件无法读取，关键数据被损坏，给用户的正常工作带来了极为严重的影响。

5 月 18 日义乌市宣传部通知：近日，全球爆发勒索蠕虫病毒，各单位要落实专人对本单位电脑进行查看，有中毒情况向市网信办汇报。同时，要组织实施人员和支持公司完成防火墙、交换机的端口关闭和系统补丁升级工作，并抓紧安装 360 等能够查杀加密勒索蠕虫的杀毒软件和专杀工具，具体关闭的端口为：TCP/UDP:135、137、138、139、9995、9996、593、445 以及 tcp:5554、4444 和 udp:1434。

2. 义乌广播的基本情况

2.1 义乌广播音频全台网情况

义乌广播采用的是英夫美迪的全台网系统（图 1），全台网内部分为播出网和制作网。为保证播出安全，广播的播出网一直在变小，一个简单高效的播出网，专注于播出更能确保播出网的安全，所以，一套节目的播出站点一般不会超过 3 台。而制作网为满足业务和发展需求，一直在变大，广播节目制作的各种要求以及面向客户、面向节目发展趋势的功能，一个大的制作系统可以满足用户的各种功能要求而不用担心功能的增加会影响到播出的安全。制作网是集节目采、编、播于一体的大制作系统，包含多媒体新闻子系统、节目制作子系统、发布子系统、媒体资产管理等多个子系统。这些子系统都围绕着节目播出这个中心，彼此协调运作。首先，新闻子系统负责新闻节目的采集、新闻稿件的生成和管理；而节目制作子系统则负责音频节的制作和管理，制作好的节目可以送往播出系统供播出使用，也可以通过发布系统发布给其他的应用系统使用。无论是新闻管理子系统还是节目制作子系统生产的节目，都可以通过内容发布子系统进行发布。除了可以发布到播出系统供播出使用外，还可以发布给其他的应用系统使用。义乌广播制作、播出系统当时设计的时候，为了便于扩容，实施的是跨网段的布署，制作网和互联网通过网闸相连(制作网和互联网以非 IP 的方式连接)，而制作站点则小部分部署在内网，大部分都布署在外网。外网制作站可以通过网闸透明的访问位于内网的制作、播出服务器，其操作和使用与位于内网的制作站完全一样。但是制作站直接布置在外网，使制作节目能调度的各种互联网素材和时效素材大大增加，对于节目的精品化和应景化有很大好处，和其他的应用系统可以通过标准的接口，直接浏览、查询制作系统的节目数据和播出系统上每套播出节目的编排情况，并能在系统授权权限许可范围内的下载使用和变更播单。系统用的媒体专用网闸，提供简化版的 HTTP、FTP、UDP 等基础协议的支持。这就能确保业务应用所必须的 webservice 应用、FTP 文件传输应用、媒资等能够顺利运行。正是有了这些中间应用的支持，制作内网、综合业务网、互联网的节目制作能透明穿透网闸，实现节目的安全、高效、协同制作。现在关闭这么多端口，哪些端口是系统在用的，也只能把交换机的端口关闭后，一步步地走节目的采编播流程。

2.2 义乌广播音频制作采编播流程和网络构架

节目编播流程：（1）用户登录制作管理软件 XStudio 系统；（2）进入我的工程区进行节目制作。新建工程，调用音频编辑器，完成音频录制编辑，发送成品节目；（3）在任务审核列表中，能够进行权限查询浏览、审核功能;（4）制作任务列表中，能够看到制作节目的审核状态；（5）发送到制作库的节目，保存在素材成品区中；（6）发送到播出库的节目，保存在播出成品区中；（7）节目发播，包括

发送到线性节目单、发送到 JINGLE 单、发送到播出成品库供查询检索播出调用。

节目编排播出除了用 XStudio 节目发播外，还能利用 LogEditor 对日播出节目单进行编排。

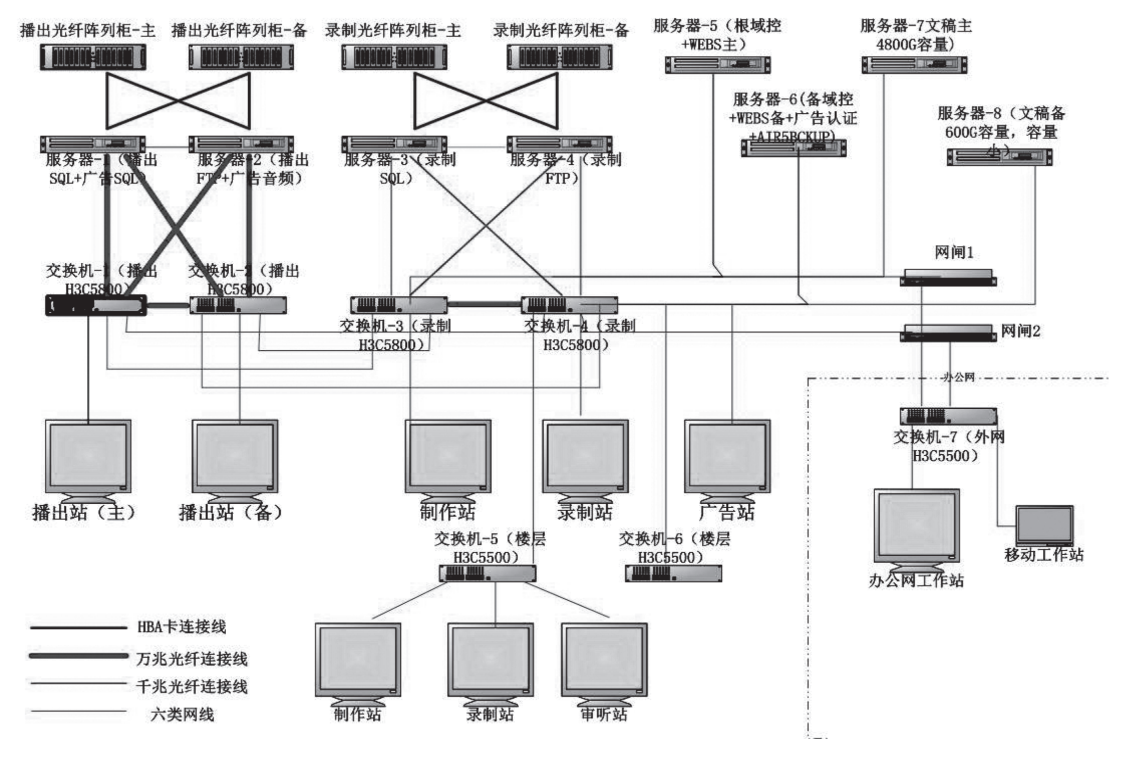


图 1　系统的网络结构图

3. 义乌广播技术应对措施

3.1 确保整个工艺流程顺利实现

广播节目所采用的素材大致分为三类：第一类是国家级的广播电视的节目、省级广播电视节目及兄弟台的广播电视节目的同期慢速录音；第二类是互联网的音频资料，包括最新的歌曲和各种声音音效；第三类自己主持人制作的精品节目和节目的文稿系统。第一类同期慢速录音采用的是联汇的 PRODS 慢速录音系统，以文件夹网络共享的方式，进行文件的访问，关闭勒索病毒传播端口后，同楼层可以访问，但是跨楼层慢录系统就读取不了文件。第二类互联网的音频资料，外网工作站往制作网传送文件的时候，走的是 HTTP，FTP 两种协议，对互联网的音频资料可以实现跨网段，跨楼层使用。第三类自己主持人制作的节目，一般在制作网内完成，不存在跨网的问题，文稿系统采用的是 HTTP 协议，关闭端口对文稿系统没有影响。解决慢录不能垮楼层使用，广播技术通过在制作网内，增加内网的工作站予以解决，这样整个广播播出的各种工艺流程在关闭勒索病毒传播端口后，通过内部测试和内部的网络结构的微调整，还是确保整个广播采制编播的顺利进行。

3.2 对网闸安全进行优化

在满足整个广播采制编播工艺流程后，广播技术对整个广播的网闸安全作了优化。

制作网和互联网之间使用 2 台 NetGap200 网闸隔离，两台网闸互做备份。2 台网闸采用并行方式，每台承担一个楼层的网络流量。NetGap200 是第二代安全网络隔离与信息交换系统网络安全产品。它把网络分为可信任网络和不可信任两部分，网闸的初始设置在可信网络端，不可信网络端只能接受和传送可信网络端给它规定的通道、端口和文件制式进行数据交换。同时数据交互通过专用的数据传输部件进行传输，对于非通道内、非端口、非合格制式的数据，系统实行高效屏蔽，可以防止各种基于网络层和操作系统层的攻击，并通过基于硬件的 SGAP 系统，实现高速实时的数据传输。网闸系统从网络模型的应用层将数据还原为原始数据，然后以“摆渡原始数据”的形式来传递数据，网络命令和 TCP/IP 协议包无法穿透隔离系统。NetGap200 还具备强大的协议终止、协议检查、内容审查等功能，可确保可信网络不受攻击，并保护网络间资源、信息和数据交换的安全进行。NetGap200 具有针对广电系统用户的特殊需求进行的优化，可根据广播的节目制作工艺要求配置允许通过的文件格式。并对要通过的音频文件进行加密和解密来实现文件传输的安全，对篡改文件名后缀、音频文件中嵌入恶意代码之类欺骗方式均能有效甄别并阻止。对于能传输进内网的文件，我们进行优化，让系统只能通过广播音频的 S48 文件。

3.3 启动多倍速快录系统并对整个制播网进行再优化

启用多倍速快录系统实现制作网和互联网的彻底的物理隔离。多倍速快录系统基本原理就是音频对录，这是一种安全又保守的做法，原来的音频对录需要人操作，多倍速快录系统就是让对录自己自动开始和停止，不需要其他的通讯机制，就依靠音频信号自身去触发。音频的开始对录、停止对录等命令，音频文件名、文件的用户名等信息，也是用音频

发电报的方式对录过去，因为正常的音频是可能以这样连续短脉冲，系统就把这样的音频短脉冲识别为编码并对其进行解析。在对录完成的音频文件中不会有这样的音频脉冲编码信号。实现了系统自动的让对录开始和停止。选择 AES3 或 MADI 进行音频对录，并采用倍速采样率的方式，比如，对于一个 48KHz 的音频文件，我们采用 192KHz 进行对录，这样对录时间可以缩短 4 倍。并且采用多通道声卡对一个文件进行同步对录，如果采用 8 个 AES3 通道的声卡，则首先将要传输的音频文件切分为 8 个音频文件，再同时将这 8 个音频文件用 8 个 AES 通道 4 倍速对录，则总的对录效率是 8×4=32 倍。义乌广播采用 64 通道 MADI，则对录效率甚至可高达 64×4=256 倍。通过这些手段，数十倍地缩短音频对录的时间，1 个小时的音频文件 1、2 分钟就完成网间传输了，而且还可以不需要人守着电脑操作，内网和外网实现彻底物理隔离，只靠音频线进行对录。

多倍速对录系统本质上是一个音频设备（图 2~3），跟其他系统的集成是以文件为唯一载体的，需要传输的音频文件只需要送到多倍速系统监测的文件夹中，多倍速系统就会自动开始对录，通过多倍速系统广播就可以轻松实现在台外的记者将音频素材传输到内网，简单的方式（图 4 多倍速系统连接简易方式）是架设 FTP 或 HTTP 服务接收音频文件传输，并将音频文件自动送多倍速，而复杂的方式（图 5 多倍速系统连接复杂方式）包括诸如将部署在外网的新闻采编系统与多倍速对录系统进行集成。这样就实现了内外网系统的彻底的物理隔离。

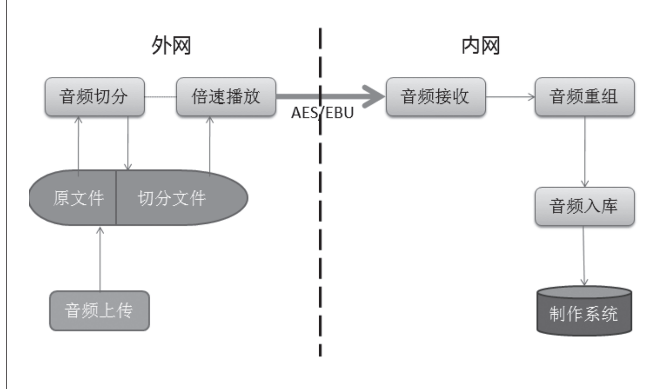


图 2 外网音频输入内网示意图

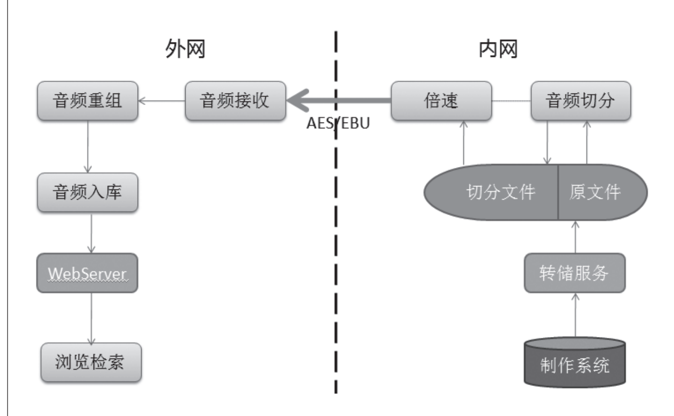


图 3 内网音频文件输出外网示意图

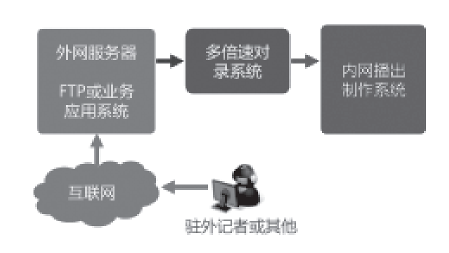


图 4 多倍速系统连接简易方式



图 5 多倍速系统连接复杂方式

在多倍速系统启用后，相对于网闸的逻辑隔离，多倍速系统的纯物理隔离在播出安全保障的级别更高，但是义乌广播技术并没有放弃网闸系统，而是让整个系统平时运行在多倍速系统中，网闸是一个备用系统，万一多倍速系统出现问题，网闸也可以发挥作用。这样义乌广播技术在网间安全保障方面拥有了多种保障手段。媒

参考文献

[1] 彭澎，何绍丹 . 基于云计算的广播制播系统研究与设计 [J]. 广播与电视技术，2013，（7）.

[2] 丁琳 .“疫情”席卷全球，它为何如此凶猛 [J]. 科学之友（上半月），2017（07）.

（作者单位：浙江省义乌广播电视传媒集团）